REMARKS

The present invention is a method of permitting access to selected information normally included in a payload of a packet upon which encrypting security processing has been performed by a node in a packet switched network during transmission of the packet to another node and a packet switched network. In accordance with the embodiment of the invention, a method includes prior to performing encrypting security processing on a payload of a packet, storing information corresponding to selected information normally included in a packet such as in a payload where, for example, transport level information including a TCP header, a user data protocol header, an Internet control message protocol header or a port number. See page 4, lines 2-5, of the specification.

The selected information is normally included in the packet in a field in a header of the packet where the field is not subject to encrypting security processing. The selected information includes transport level information which is usable by at least one intermediate node between the node and another node in the packet switched network to provide value added services relative to transmission. See page 4, lines 24-26 through page 5, lines 1-18, of the specification.

The present invention permits access to the selected information normally included in the payload of a packet upon which encrypting security processing has been performed as, for example by utilizing of the sequence control field of a security protocol header to convey information related to the selected information when security processing has been performed. See, for example, page 14, lines 12-21, of the specification.

In the Advisory Action of November 17, 2004, the Examiner states as follows:

> Applicant has argued against this combination by stating that Levesque and Denker fail to teach "prior to encrypting security processing on a payload of a packet, storing information corresponding to selected information normally included in a payload of the packet in a field in a header of the packet where the field is not subject to encrypting security processing, the selected information including transport level information usable by intermediate nodes between a sending node and a receiving node to provide value added services relative to the transmission." Examiner respectfully disagrees. Levesque teaches the storing of information in the header of the packet, prior to encrypting security processing, where the field is not subject to encrypting security processing (Levesque, column 3 lines 22-25, header loaded before security network driver issues an encryption call). Denker teaches that the transport level information usable by intermediate nodes between a sending node and a receiving node is used to provide value added services relative to the transmission (Denker, column 3 lines 25-65, port number placed in sequence number field). Applicant has argued on Page 4 that Denker does not suggest that a port number is normally included in the payload of a packet. Examiner notes that a port number is data that is normally included in a TCP packet. TCP packets are found in the payload of IP packets and thus, the inclusion of a port number in the sequence number field of a packet header is an example of including transport level information normally included in the payload of a packet in the header of a packet. Examiner has provided "TCP/IP Suite" by Protocols.com to show evidence of a port number being normally included in the payload of a packet (see Page 3 - Data and Page 6 TCP). The transport level information that Denker includes is usable by an intermediate node for the value-added service of preventing SYN attacks (Denker, column 3 lines 25-30) or providing methods of recognizing and shutting down halt open connections (Denker, column 3 lines 51-55). By preventing SYN attacks, intermediate nodes provide the value-added service of policing.

Claims 1, 4, 11 and 14 stand rejected under 35 U.S.C. §103 as being unpatentable over United States Patent 5,825,891 (Levesque et al) in view of United States Patent 5,958,053 (Denker). With respect to claims 1 and 11 the Examiner reasons as follows:

> With regards to claims I and 11, Levesque teaches that prior to performing encryption on the payload of the packet, information is stored in the header that is not subjected to encrypting security processing (Levesque, column 3 lines 28-39). Levesque further teaches performing encrypting security processing on the payload of the packet (Levesque, column 3, lines 40-45), transmitting the packet including the header and the payload upon which encrypting security processing has been performed in the packet switched

network thereby permitting access to the selected information normally included in the payload of the packet via the header of the packet by a node in the packet switched network (Levesque, column 3, lines 63-65). Levesque fails to teach the selected information including transport level information where the transport level information is useable by intermediate nodes between the node and another node in the packet switched network to provide value added services relative to the transmission. Denker teaches the selected information including transport level information (Denker, column 3 lines 25-39 and lines 52-59, "port number") where the transport level information is useable by intermediate nodes between the node and another node in the packet switched network to provide value added services relative to the transmission (Denker, column 3 lines 25-50, value added services in the form of authentication by matching hash values or policing). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Denker's method of encoding transport level information into packet headers with Levesque's key management system because it offers the advantage of adding additional security abilities to the communication system such as the ability to resist SYN floods (Denker, column 3 lines 6-27).

These grounds of rejection are traversed for the following reasons.

In the first place, the Examiner correctly acknowledges in the Final Rejection discussion of claims 1 and 11 as set forth above that Levesque et al fail to teach that the selected information, which is encrypted, includes transport level information where the transport level is usable by intermediate nodes between the node and another node in the packet switched network to provide value added services. However, the Examiner has impermissibly broadened the definition of value added services to be a specification of a port number *per se*. It is submitted that a port number would not be considered by a person of ordinary skill in the art to be a value added service.

Denker, in column 3, lines 25-65, describes a defense to synchronization flag (SYN) flooding which is known as the syncookie method. What is described in the referenced portions of Denker in column 3, lines 52-59, is that the Initial Sequence Number ($c) "should

include, to a significant approximation, the source IP address and port number, and (if possible) an all important information carried by the option (OPT) fields in the original SYN message". It is submitted that reference to a sequence number $c, which is generated by the server as a cryptographic function as described in column 3, lines 25-50, is not anything more than a specification of the sequence number which would not be understood by a person of ordinary skill in the art to be the claimed value added service. If the Examiner persists in the stated grounds of rejection, even though patent claims are to be given their broadest reasonable interpretation by a person of ordinary skill in the art, it is submitted that the Examiner has not demonstrated that applying that standard that a port number is a value added service.

In this regard, it is noted that the Examiner has stated that amended claim 3 specifies that port number information is a form of transport level information as defined by Applicant. However, amended claim 3 defines the scope of transport level information as recited in claim 1, but it is submitted that claim 3 by defining transport level information as including port number information does not admit anything regarding the utilization of, as recited in the independent claims, "said transport level information being usable by at least one intermediate nodes between said node and said another node in the packet switched network to provide value added services relative to the transmission". As stated above, the specifying of a port number per se is not a value added service as understood by a person of ordinary skill in the art.

Moreover, it is submitted that the Examiner has not demonstrated any basis in the record why a person of ordinary skill in the art would be motivated to combine

Levesque et al's teachings with Denker. The Examiner's conclusion that motivation to combine is demonstrated is stated to be that "Denker's method...offers the advantage of adding additional security abilities to the communications system such as the ability to resist SYN floods." However, SYN floods have nothing to do with value added services and are intended to avoid flooding of a network which is outside the scope of the claimed value added services. Accordingly, it is submitted that there is no motivation in the record regarding the claimed "selected information including transport level information, said transport level information being usable by at least one intermediate node between said node and said another node in the packet switched network to provide value added services relative to the transmission" as recited in independent claims 1 and 11. The only basis to utilize transport level information for providing value added services is by impermissible hindsight. Dependent claims 4 and 14 are patentable for the same reasons set forth above with respect to claims 1 and 11.

It is noted that the Examiner discusses claims 2 and 12 in Section 10 of the Office Action which it is assumed were intended to be rejected on the grounds of obviousness over Levesque and Denker. In any event, the Examiner cites column 3, lines 25-50, as providing value added services in the form of authentication by matching hash values or policing. The reference therein to matching hash values to the appropriate function output is submitted to not describe a value added service.

Independent claims 21-26 are specific to the value added services comprising at least one of differentiated services, policing at least one of the nodes and management of nodes for metering as disclosed on page 5 of the specification. It is submitted that this subject

17

matter is not suggested in Denker in column 3, lines 25-50. Moreover, there is no basis why a person of ordinary skill in the art would be led to modify the teachings of Levesque and Denker to arrive at this subject matter.

Furthermore, it is noted that the Examiner further discusses claims 3-8 and 13-18 in Sections 11-15 of the Office Action. It is understood that the Examiner intended to reject those claims on the combination of Levesque et al and Denker et al. It is submitted that these claims are patentable for the reasons set forth above with respect to a proposed combination of Levesque and Denker as discussed with respect to claims 1 and 11.

Claims 9-10 and 19-20 stand rejected under 35 U.S.C. §103 as being unpatentable over Levesque and Denker further in view of RFC 2401 (Atkinson et al). Atkinson et al has been cited as teaching the use of ESP and AH in IP security. However, this does not cure the deficiencies noted above with respect to the proposed combination of Levesque and Denker et al.

In view of the foregoing amendments and remarks, it is submitted that each of the claims in the application is in condition for allowance. Accordingly, early allowance thereof is respectfully requested.
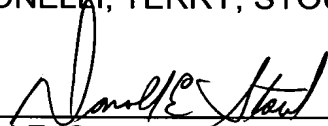
To the extent necessary, Applicants petition for an extension of time under 37 FR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the

Deposit Account of Antonelli, Terry, Stout & Kraus, LLP, Deposit Account No. 01-2135

(referencing attorney docket no. 0173.37334X00).Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Donald E. Stout
Registration No. 26,422
(703) 312-6600

DES:dlh